Microsoft

Role of AI in Cybersecurity

Ashish K Adhikari
Microsoft Engineering – CyberSecurity

Industry Trends

65% of organizations reported a with 59% reporting .

—**(ISC)^2** *Cybersecurity Workforce Study*

Customers spend and found a disapprovingly meager 26% of cases reported through the SOC.

—**EY** *Global information security survey 2020*

Roughly 50% of SOCs and 43% of SOCs report an due to a lack of integrated security tools.

—**SANS** *Common and Best Practices for Security Operations Centers:*
Results of the 2019 SOC Survey

26% of businesses have seen an since 12 March 2020.

—**CSO** *Pandemic Impact Survey March 2020*

Information security is in transformation

Enterprise IT is Cloud Hybrid

Cloud adoption is inevitable (digital transformation + industry momentum).

Legacy systems will take years to migrate or retire.

Technology Mobility and Volume is Exploding

Increasing demand for first class experience on mobile devices.

Variance in trustworthiness of mobile devices.

Pervasive Digital Transformation and IoT

IoT adoption driving a wave of app development and cloud usage.

Enterprise PC security strategies applying poorly to IoT devices.

Increasingly Hostile Environment

Increased attack surface with updated technologies creates new blind spots.

Attacks rising in volume and sophistication to capture illicit opportunities.

Note Attackers generally invest in technical sophistication only as needed.

O365 Software

AI and automation to secure your future

Built-in experiences across platforms

"Some of our users haven't even noticed that we implemented enhanced security features. I think that's the best way to implement security—seamlessly and in the background."

Forrester found that Microsoft security technology automatically remediates 97% of endpoint attacks detected, freeing up teams to resolve the most complicated cases.

Best in class and integrated

Deliver integrated coverage across your entire environment, from Endpoint Security to CASB to Zero Trust and everything in between.

Microsoft Intelligent Security pillars

Identity and Access Management

Manage and secure identities on a universal platform

Threat Protection

Stop attacks with integrated and automated security – Anti Virus and EDR.

Email Security

Protect your incoming and outgoing email communications.

Cloud Security

Safeguard your cross-cloud resources.

Compliance Pillars

Information Protection and Governance

Protect and govern your Data whenever it lies

Insider Risk Management

Identify and take action on critical insider risks

Discover and Respond

Quickly investigate and respond with relevant data

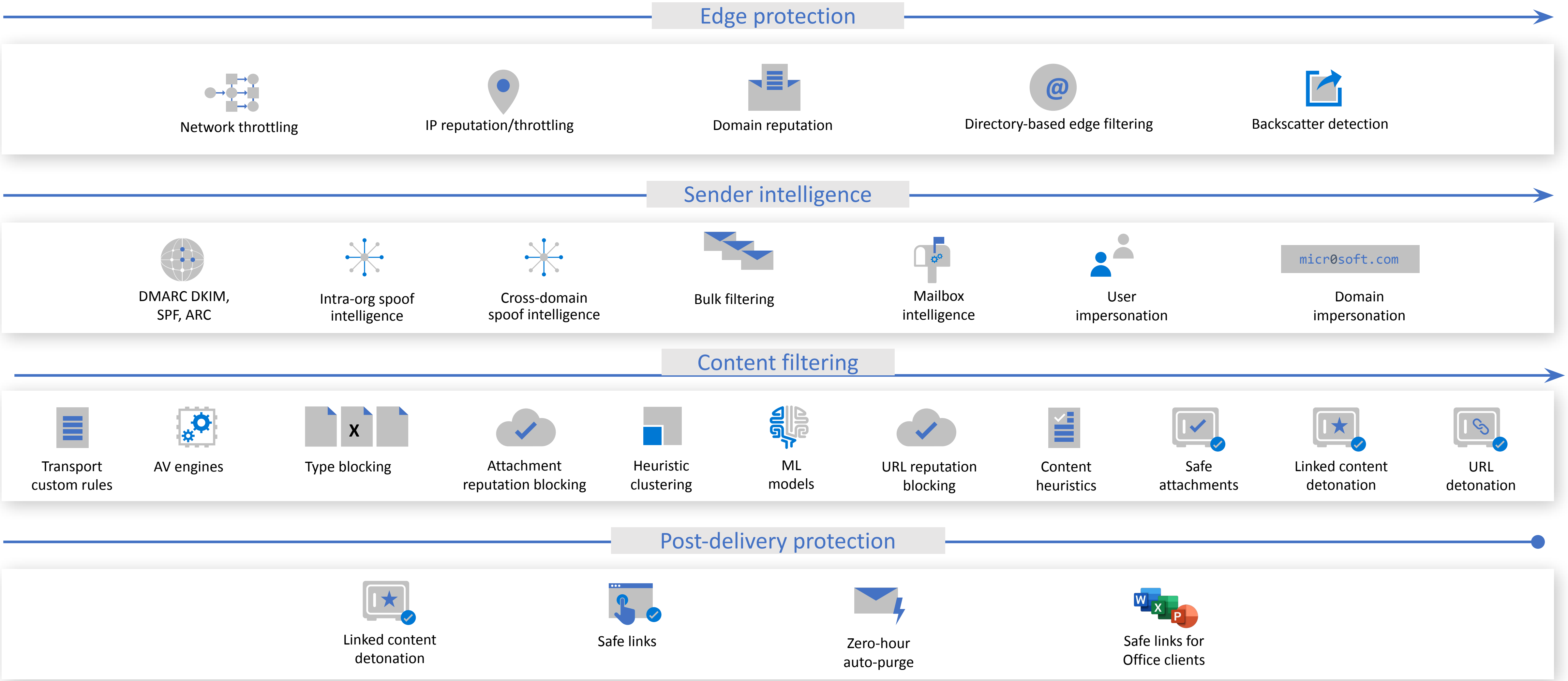
Compliance Management

Simplify Compliance and reduce risk

Microsoft

Use of AI in Email filtering

How much time does it takes for email to reach from Person A , to Person B ?



Edge protection

Network throttling

IP reputation/throttling

Domain reputation

Directory-based edge filtering

Backscatter detection

Sender intelligence

DMARC DKIM, SPF, ARC

Intra-org spoof intelligence

Cross-domain spoof intelligence

Bulk filtering

Mailbox intelligence

User impersonation

micr0soft.com

Domain impersonation

Content filtering

Transport custom rules

AV engines

X

Type blocking

Attachment reputation blocking

Heuristic clustering

ML models

URL reputation blocking

Content heuristics

Safe attachments

Linked content detonation

URL detonation

Post-delivery protection

Linked content detonation

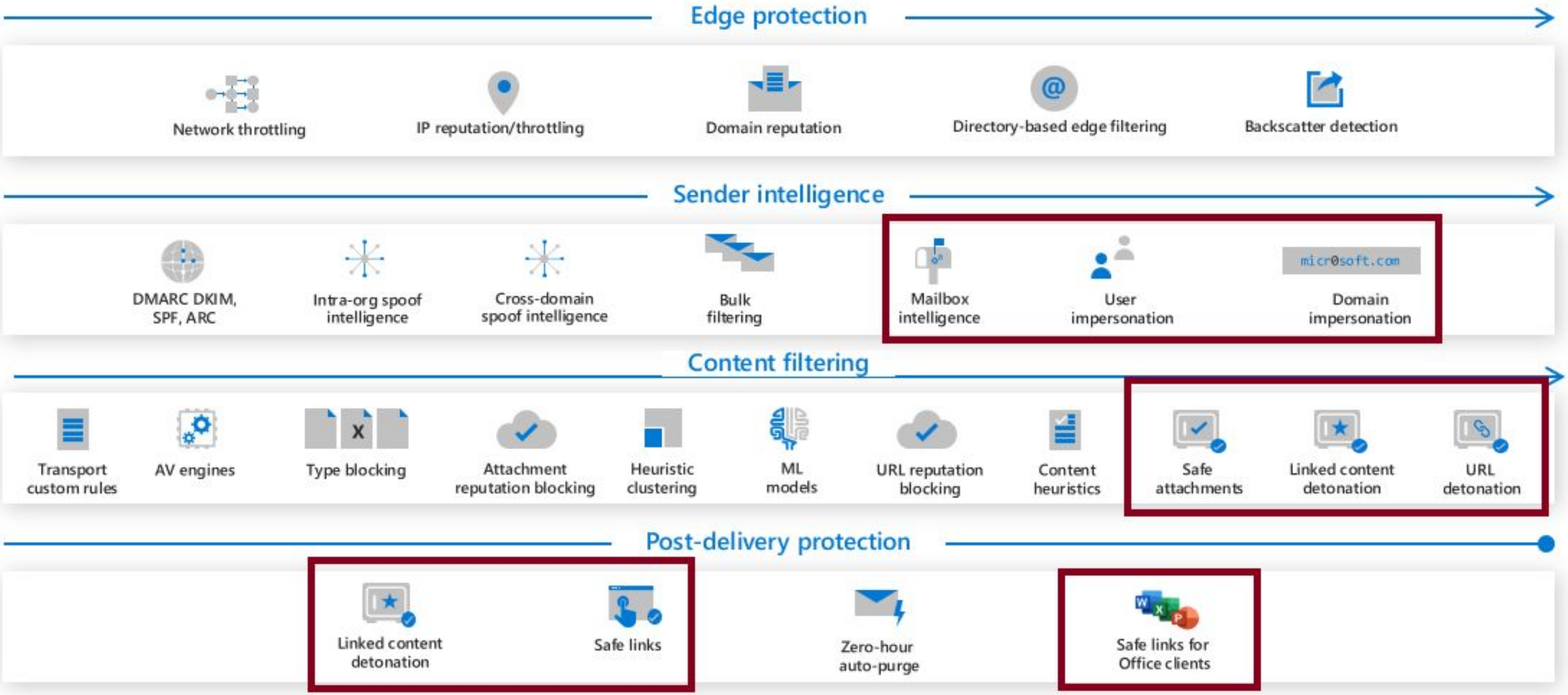
Safe links

Zero-hour auto-purge

W X P

Safe links for Office clients

Massive leverage of AI at each filter



Edge protection

Network throttling

IP reputation/throttling

Domain reputation

Directory-based edge filtering

Backscatter detection

Sender intelligence

DMARC DKIM, SPF, ARC

Intra-org spoof intelligence

Cross-domain spoof intelligence

Bulk filtering

Mailbox intelligence

User impersonation

micr0soft.com

Domain impersonation

Content filtering

Transport custom rules

AV engines

Type blocking

Attachment reputation blocking

Heuristic clustering

ML models

URL reputation blocking

Content heuristics

Safe attachments

Linked content detonation

URL detonation

Post-delivery protection

Linked content detonation

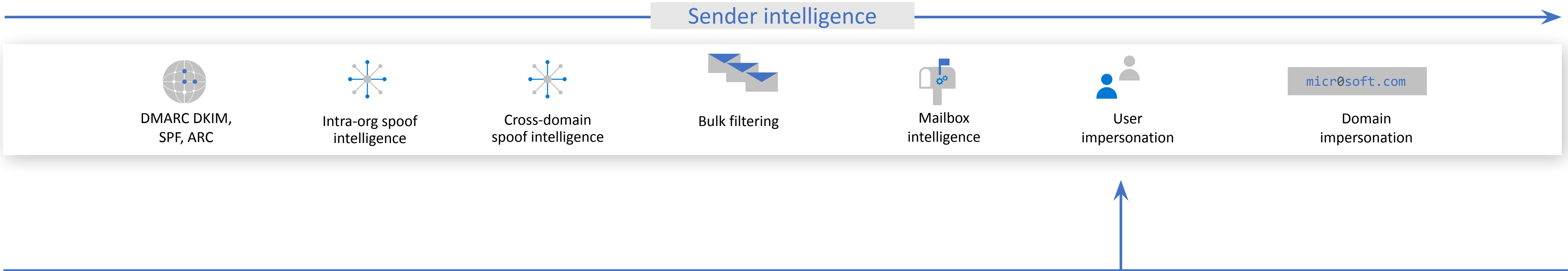
Safe links

Zero-hour auto-purge

Safe links for Office clients

Microsoft

Email and AI- few more scenarios



Sender intelligence

DMARC DKIM, SPF, ARC

Intra-org spoof intelligence

Cross-domain spoof intelligence

Bulk filtering

Mailbox intelligence

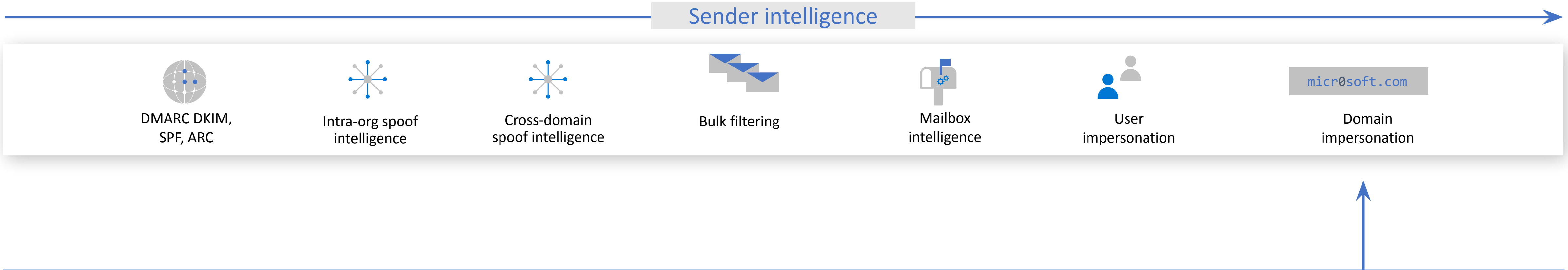
User impersonation

micr0soft.com

Domain impersonation

User impersonation allows an admin to provide a list of high value targets that are likely to be impersonated within their organization. If a mail arrives with a sender with the same name, but a different address the recipient is warned.

It uses complex algorithm to make combination of defined display names in **“users to protect”** list, which also include similar sounding and abbreviated names



Sender intelligence

DMARC DKIM, SPF, ARC

Intra-org spoof intelligence

Cross-domain spoof intelligence

Bulk filtering

Mailbox intelligence

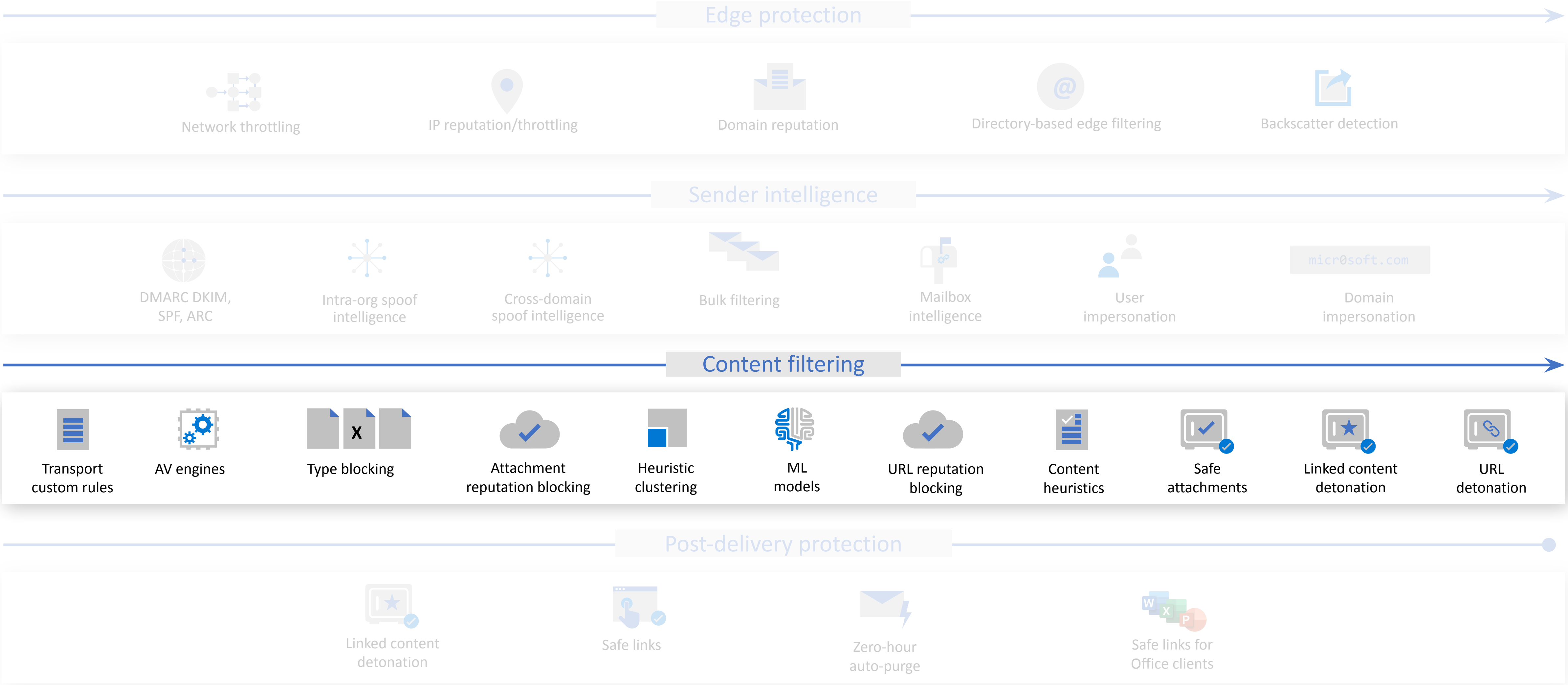
User impersonation

micr0soft.com

Domain impersonation

Domain impersonation detect domains that are similar to the recipient’s domain, attempting to look like an internal domain.

It uses complex algorithm to make combination of similar domain names based on accepted domains which are part of an organization



Edge protection

Network throttling

IP reputation/throttling

Domain reputation

Directory-based edge filtering

Backscatter detection

Sender intelligence

DMARC DKIM, SPF, ARC

Intra-org spoof intelligence

Cross-domain spoof intelligence

Bulk filtering

Mailbox intelligence

User impersonation

micr0soft.com

Domain impersonation

Content filtering

Transport custom rules

AV engines

Type blocking

Attachment reputation blocking

Heuristic clustering

ML models

URL reputation blocking

Content heuristics

Safe attachments

Linked content detonation

URL detonation

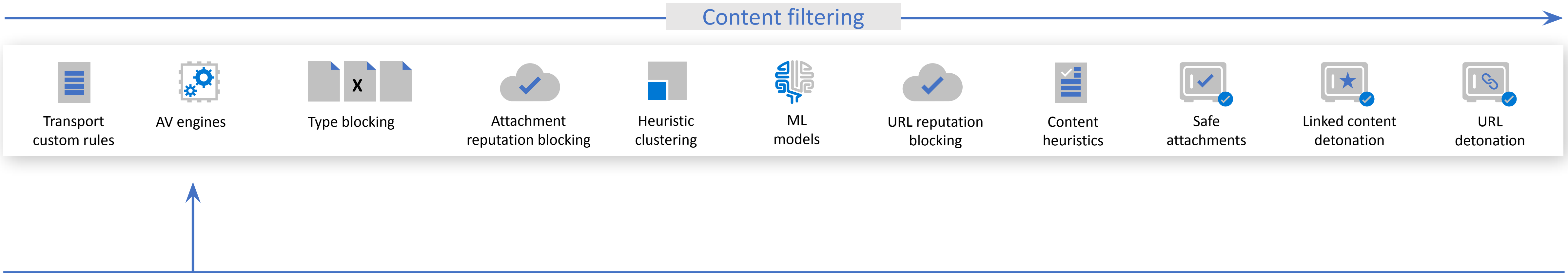
Post-delivery protection

Linked content detonation

Safe links

Zero-hour auto-purge

Safe links for Office clients



Content filtering

Transport custom rules

AV engines

Type blocking

Attachment reputation blocking

Heuristic clustering

ML models

URL reputation blocking

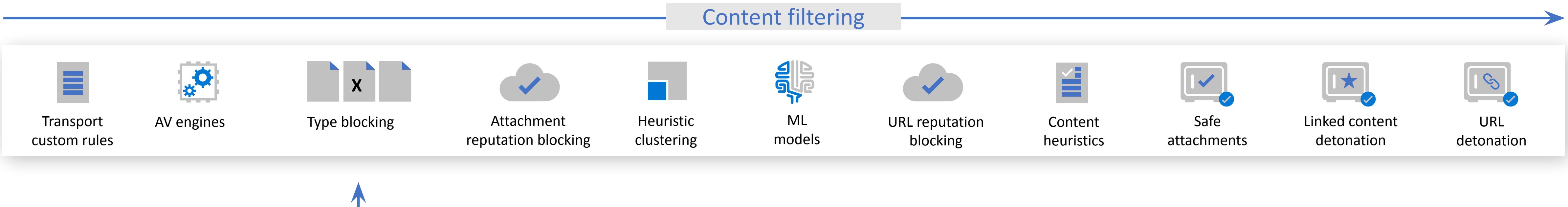
Content heuristics

Safe attachments

Linked content detonation

URL detonation

MSAV and two third-party **AV engines** are used to detect all known malware in attachments.



Content filtering

Transport custom rules

AV engines

Type blocking

Attachment reputation blocking

Heuristic clustering

ML models

URL reputation blocking

Content heuristics

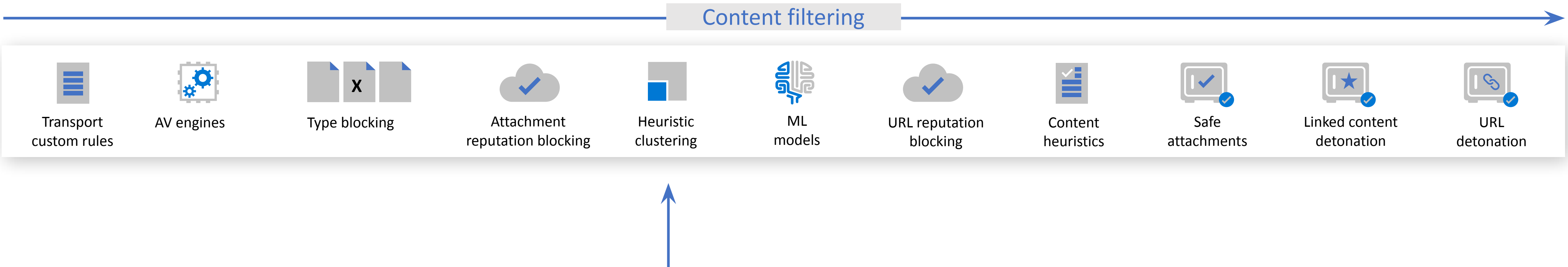
Safe attachments

Linked content detonation

URL detonation

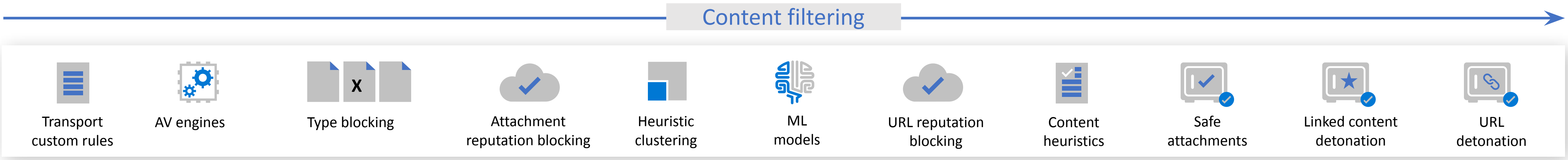
The AV engines are also used to true-type all attachments so that **type blocking** can block all attachment of the types the admin specifies.

It uses ML to filter out FNs



Heuristic clustering can determine that a file is suspicious based on delivery heuristics. When a suspicious attachment is found the entire campaign is paused and the file is sandboxed. If it is found to be malicious the entire campaign is blocked.

It uses ML to filter out FNs



Content filtering

Transport custom rules

AV engines

Type blocking

Attachment reputation blocking

Heuristic clustering

ML models

URL reputation blocking

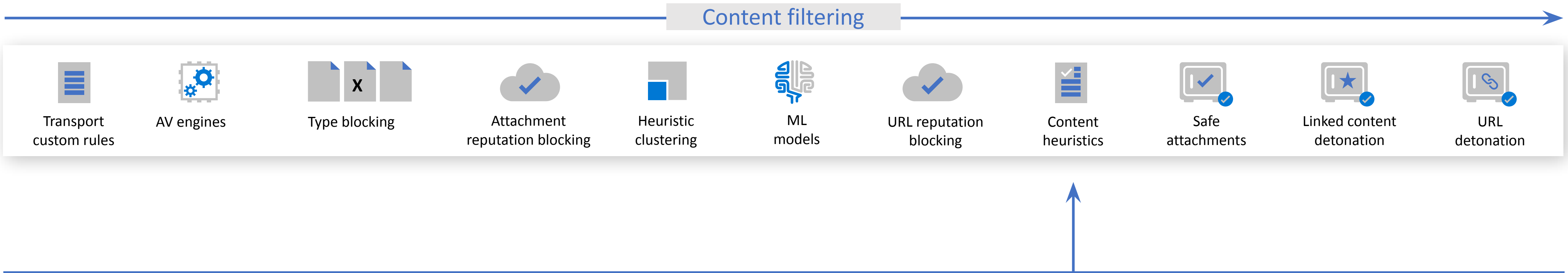
Content heuristics

Safe attachments

Linked content detonation

URL detonation

Machine learning models act on the header, body content, and URLs of a message to detect phishing attempts.



Content filtering

- Transport custom rules
- AV engines
- Type blocking
- Attachment reputation blocking
- Heuristic clustering
- ML models
- URL reputation blocking
- Content heuristics
- Safe attachments
- Linked content detonation
- URL detonation

Content heuristics can detect suspicious messages based on structure and word frequency within the body of the message using machine learning models.

It uses ML to filter out FNs

Microsoft 365 Security and Compliance Suite Value

Built-in experiences across platforms

"Some of our users haven't even noticed that we implemented enhanced security features. I think that's the best way to implement security—seamlessly and in the background."

AI and automation to secure your future

Forrester found that Microsoft security technology automatically remediates 97% of endpoint attacks detected, freeing up teams to resolve the most complicated cases.

Best in class and integrated

Deliver integrated coverage across your entire environment,
from Endpoint Security to CASB
to Zero Trust and everything in between.

Microsoft Intelligent Security pillars

Identity and Access Management

Manage and secure identities on a universal platform

Threat Protection

Stop attacks with integrated and automated security – Anti Virus and EDR.

Email Security

Protect your incoming and outgoing email communications.

Cloud Security

Safeguard your cross-cloud resources

Compliance Pillars

Information Protection and Governance

Protect and govern your Data whenever it lies

Insider Risk Management

Identify and take action on critical insider risks

Discover and Respond

Quickly investigate and respond with relevant data

Compliance Management

Simplify Compliance and reduce risk

Lets see what's sensitive in a School ?

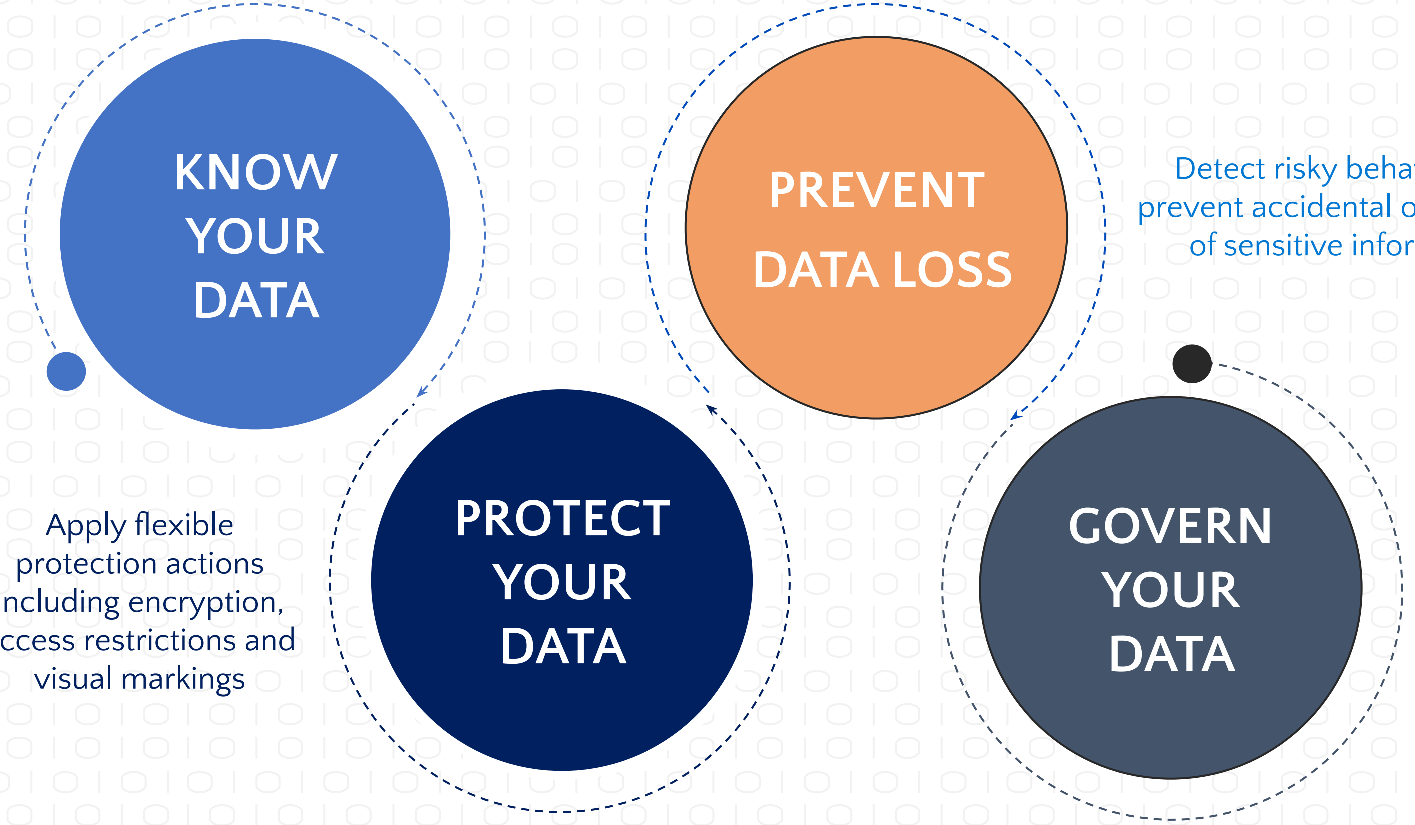
Do you know where your student data, Exams yet to be taken and sensitive data resides and what is being done with it?

Do you have control of this data as it travels inside and outside of your organization?
Exam leak comes to mind ?

Are you using multiple solutions to classify, label, and protect this data?

Information Protection & Governance

Protect and govern data – **wherever** it lives



KNOW YOUR DATA

Understand your data landscape and identify important data across your hybrid environment

PROTECT YOUR DATA

Apply flexible protection actions including encryption, access restrictions and visual markings

PREVENT DATA LOSS

Detect risky behavior and prevent accidental oversharing of sensitive information

GOVERN YOUR DATA

Automatically retain, delete, and store data and records in a compliant manner

Powered by an intelligent platform

Unified approach to automatic data classification, policy management, analytics and APIs

Can system recognize ?
Tax documents Vs Exam paper

Built-in ready-to-use models

+

Build your own models

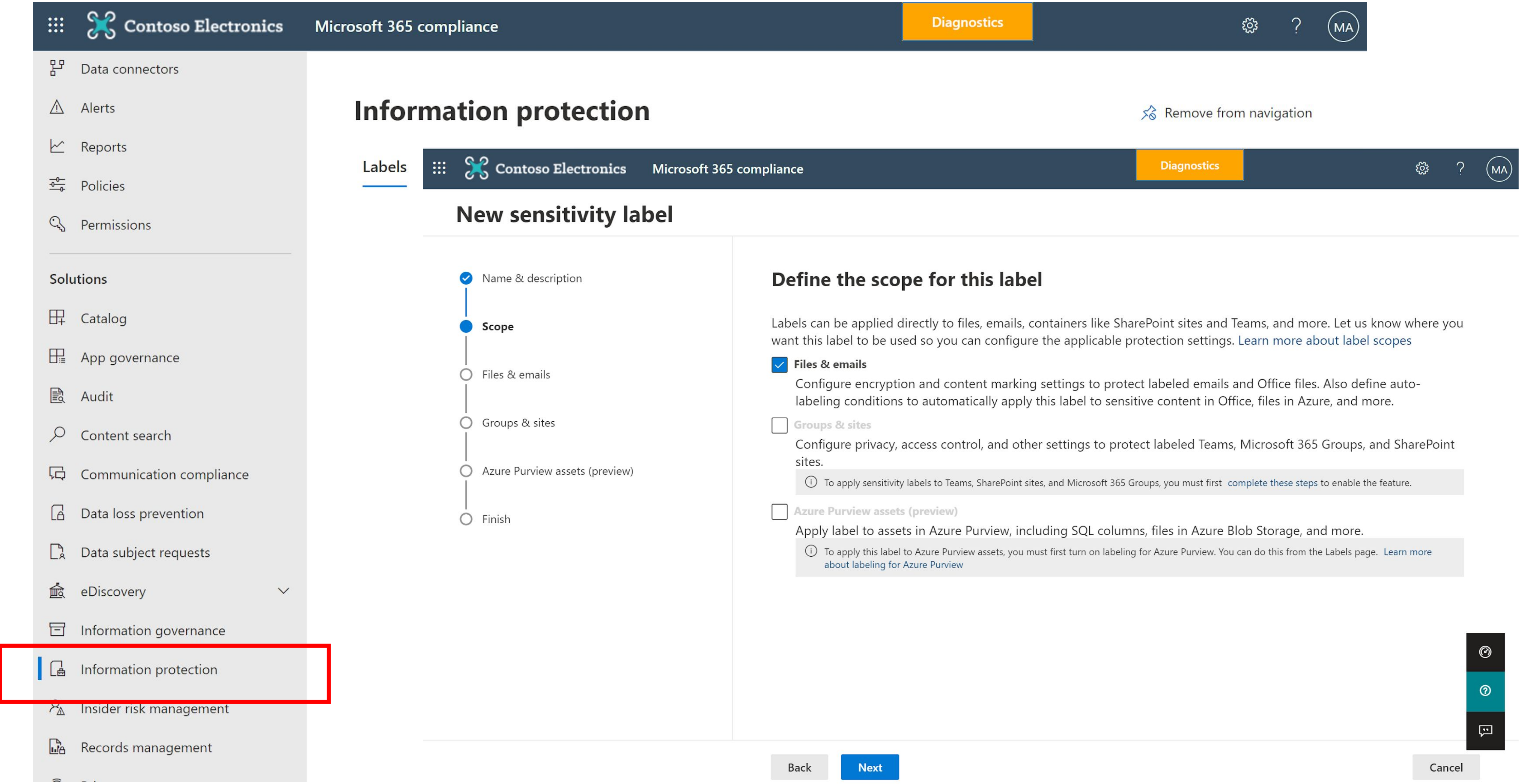
Microsoft built-in models ready-to-use models which don’t require any training

Custom models which can be seeded, tested and trained on customer data

Current list of ready-to-use models

Classifier	Language	Use case
Source Code	English	Information protection, data loss prevention, information governance
Resume	English	Information protection, data loss prevention, information governance
Threat	8 tier-1 languages	Communication compliance
Profanity	8 tier- 1 languages	Communication compliance
Harassment	8 tier- 1 languages	Communication compliance

Workflow – OOB models



Information protection

New sensitivity label

Define the scope for this label

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. Learn more about label scopes

☑ **Files & emails**

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

☐ **Groups & sites**

Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

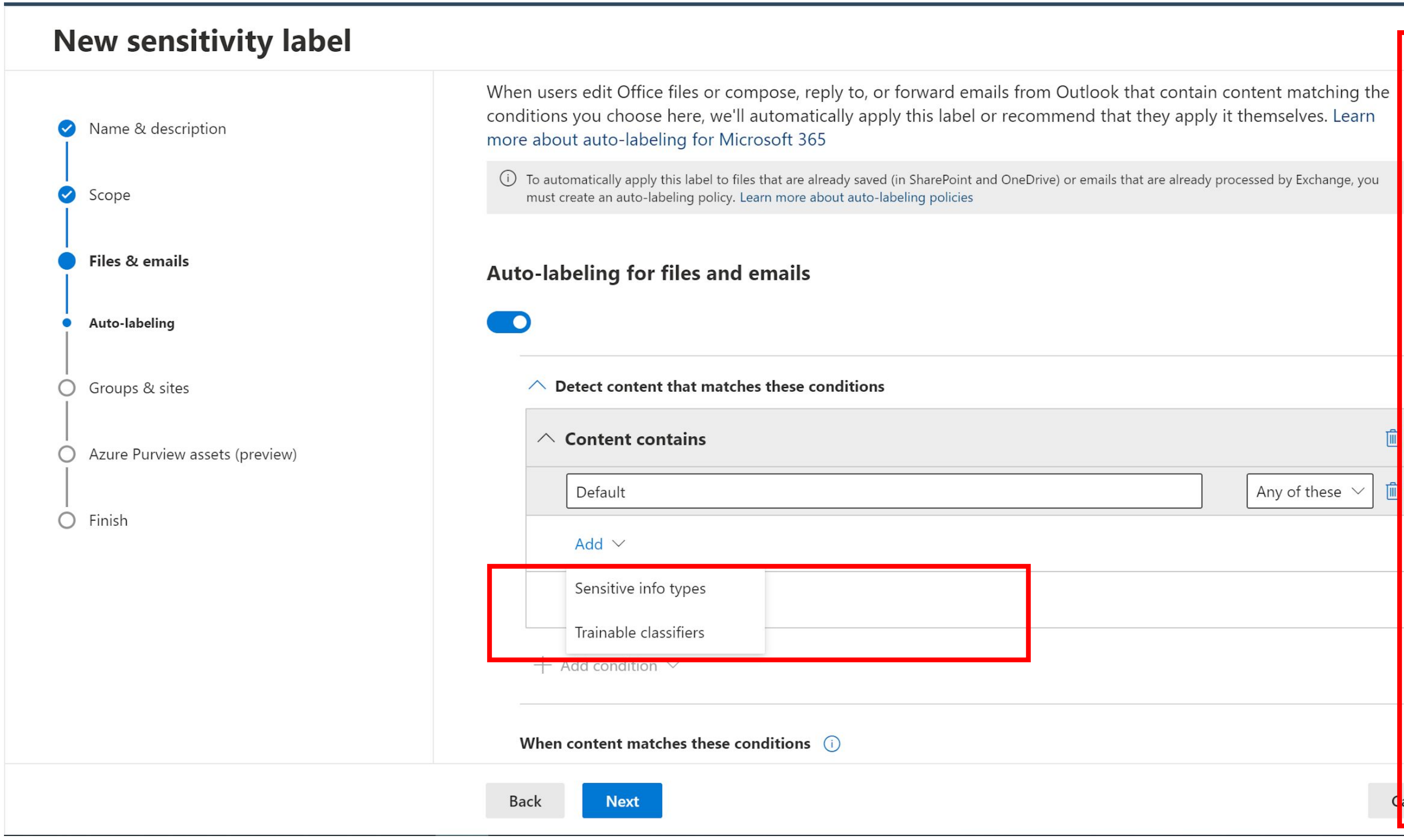
ⓘ To apply sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first complete these steps to enable the feature.

☐ **Azure Purview assets (preview)**

Apply label to assets in Azure Purview, including SQL columns, files in Azure Blob Storage, and more.

ⓘ To apply this label to Azure Purview assets, you must first turn on labeling for Azure Purview. You can do this from the Labels page. Learn more about labeling for Azure Purview

Workflow – OOB models



New sensitivity label

- Name & description
- Scope
- **Files & emails**
- **Auto-labeling**
- Groups & sites
- Azure Purview assets (preview)
- Finish

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling for Microsoft 365

To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. Learn more about auto-labeling policies

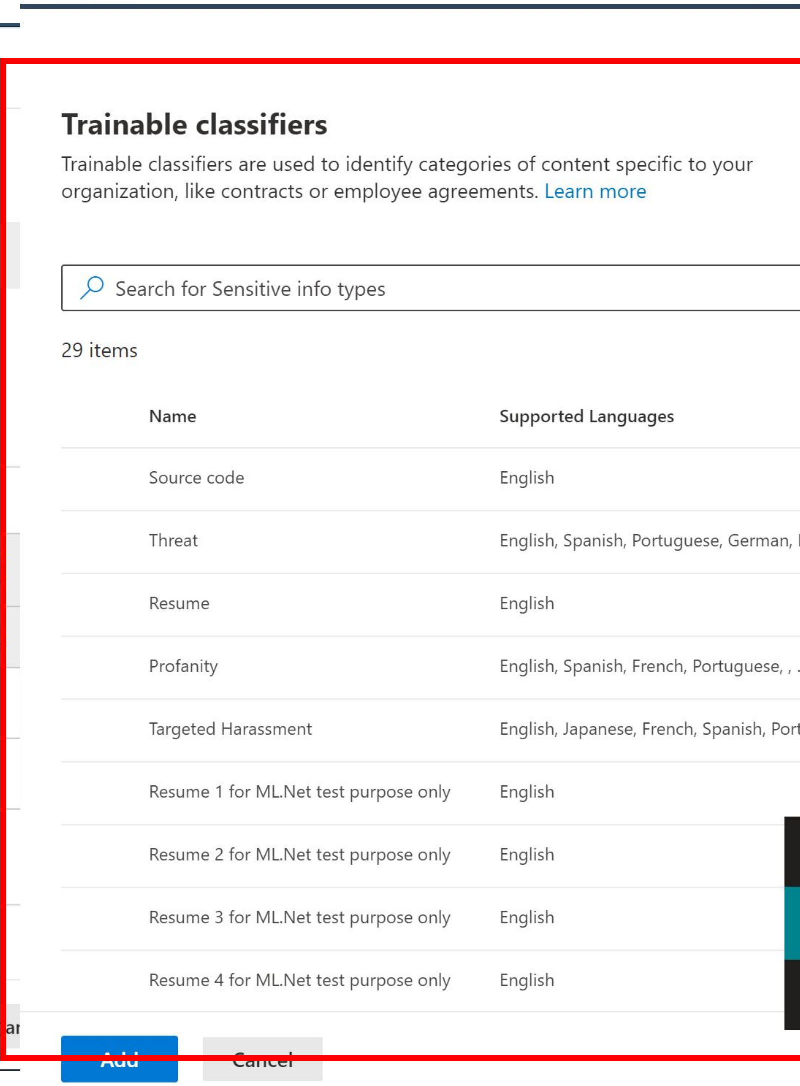
Auto-labeling for files and emails

Detect content that matches these conditions

Content contains

Default — Any of these

When content matches these conditions



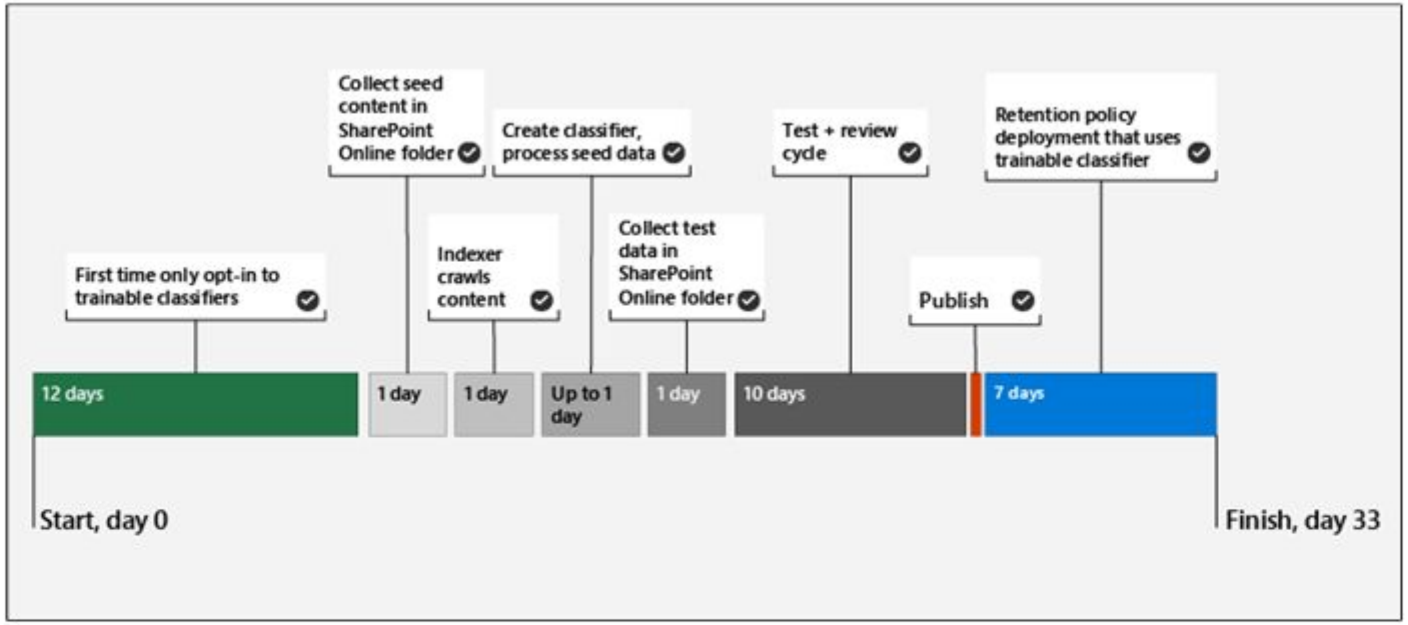
Trainable classifiers

Trainable classifiers are used to identify categories of content specific to your organization, like contracts or employee agreements. Learn more

29 items

Name	Supported Languages
Source code	English
Threat	English, Spanish, Portuguese, German,
Resume	English
Profanity	English, Spanish, French, Portuguese, ,
Targeted Harassment	English, Japanese, French, Spanish, Por
Resume 1 for ML.Net test purpose only	English
Resume 2 for ML.Net test purpose only	English
Resume 3 for ML.Net test purpose only	English
Resume 4 for ML.Net test purpose only	English

Workflow – Custom Trainable Classifiers



First time only opt-in to trainable classifiers

Collect seed content in SharePoint Online folder

Indexer crawls content

Create classifier, process seed data

Collect test data in SharePoint Online folder

Test + review cycle

Publish

Retention policy deployment that uses trainable classifier

12 days

1 day

1 day

Up to 1 day

1 day

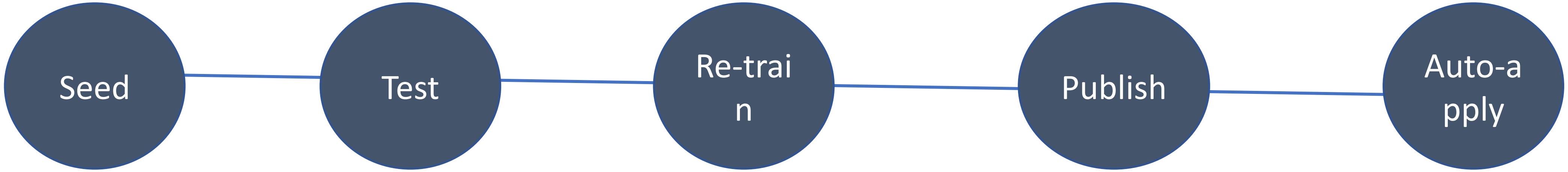
10 days

7 days

Start, day 0

Finish, day 33

1. Min 50 seed documents most related to category (Positive samples)
2. Min 200 items for testing (Positive + negative + combined)
3. Grade match/no-match in #2
4. Train till desired accuracy is achieved



Seed

Test

Re-train

Publish

Auto-apply

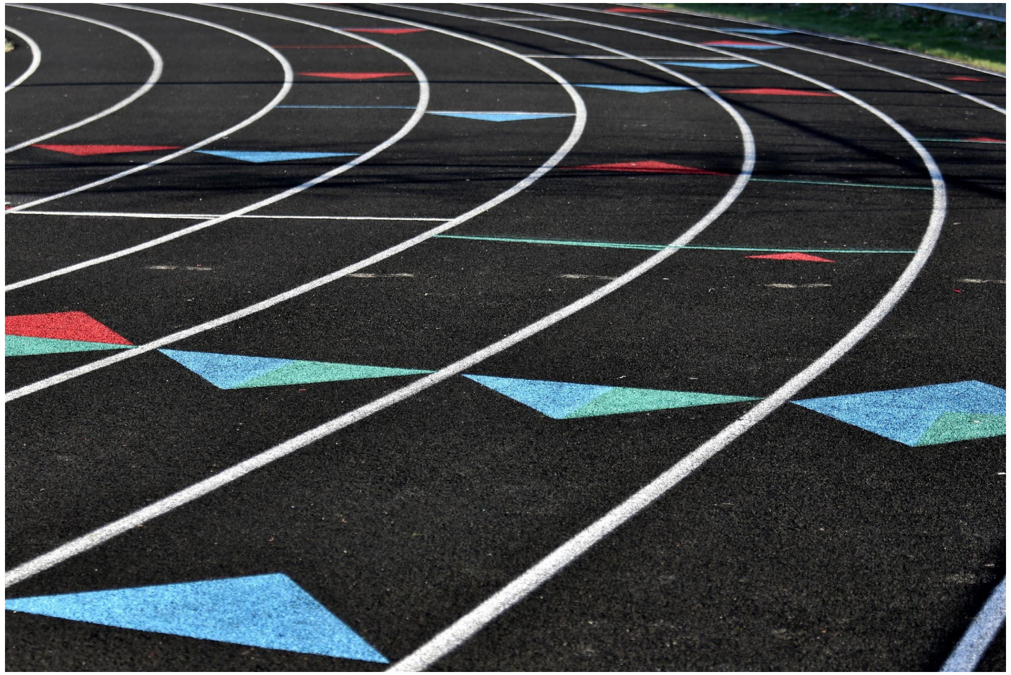
Trainable Classifiers – Roadmap

9 Broad Business Category Models
(Finance, IT, IP, Contracts, HR, Healthcare, Legal, Tax, Patent, Procurement) in Private Preview and GA in next 6 months

~15 New OOB Ready-to-use Models
Customer voted top categories
Click here to share your priority with us:

Simplify Custom Models
Make it easier to train and deploy with pre-labeled data

Many More capabilities
- Trainable Classifiers in DLP, IRM (Private preview only)
- Discovery without Labeling



Challenge #1 – Try building Exam Classifier in your O365 system and detect whats going on in your IT environment.

Questions?

Microsoft

Thank you!